DCIT 409 – DIGITAL FORENSICS

GROUP ASSIGNMENT

MEMBERS :

1. Paul Woolley 10921657

2. Hertha Fredina Gobr - 10888653

3. Ransford Gyasi - 10869753

4. Solomon Andoh - 10908662

5. Joseph Opoku Boadu - 10897994

6. Nhyira Swanzy - 10916117

7. Osei-Owusu Nana Yaw - 10916524

8. Sitsofe Abena Agorsu-Atsu - 10893106

9. Lois Osei Ampofo-10904963

10. Kwame Okyere Addo - 10921580

QUESTION 1

a. **strace**:

It is a useful diagnostic, instructional, and debugging tool. System administrators, diagnosticians and trouble-shooters will find it invaluable for solving problems with programs for which the source is not readily available since they do not need to be recompiled in order to trace them. It intercepts and records the system calls which are called by a process and the signals which are received by a process. Captures and records system calls made by a running process, allowing in-depth analysis of its interactions with the kernel. Useful for debugging and understanding program behavior at a system call level.

b. **uptime**:

uptime gives a one line display of the following information. The current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes. System load averages is the average number of processes that are either in a runnable or uninterruptable state. A process in a runnable state is either using the CPU or waiting to use the CPU.

c. **ss**:

It is used to dump socket statistics. It allows showing information similar to netstat. It can display more TCP and state information than other tools. It is a utility to investigate sockets. When no option is used ss displays a list of open non-listening sockets (e.g. TCP/UNIX/UDP) that have established connection.

d. **netstat**:

Netstat is a versatile command-line tool that displays various network-related information. It is instrumental in examining active network connections, routing tables, interface statistics, masquerade connections and multicast memberships. It prints information about the Linux networking subsystem.

e. **vmsta**t:

Virtual memory statistics reporter, also known as vmstat, is a Linux command-line tool that reports various bits of system information. Things like memory, paging, processes, IO, CPU, and disk scheduling are all included in the array of information provided. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length delay. The process and memory reports are instantaneous in either case.

f. **top**:

This command displays Linux processes. The top program provides a dynamic real-time view of a running system. It can display system summary information as well as a list of processes or threads currently being managed by the Linux kernel. The types of system summary information shown and the types, order and size of information displayed for processes are all user configurable and that configuration can be made persistent across restarts. The program provides a limited interactive interface for process manipulation as well as a much more extensive interface for personal configuration -- encompassing every aspect of its operation. And while top is referred to throughout this document, you are free to name the program anything you wish. That new name, possibly an alias, will then be reflected on top's display and used when reading and writing a configuration file.

g. **htop**:

htop is a cross-platform ncurses-based process viewer. It is similar to top, but allows you to scroll vertically and horizontally, and interact using a pointing device (mouse). You can observe all processes running on the system, along with their command line arguments, as well as view them in a tree format, select multiple processes and act on them all at once. Tasks related to processes (killing, renicing) can be done without entering their PIDs.

h. **tcpdump**:

tcpdump is a command-line utility that you can use to capture and inspect network traffic going to and from your system. It is the most commonly used tool among network administrators for troubleshooting network issues and security testing. Despite its name, with tcpdump, you can also capture non-TCP traffic such as UDP, ARP, or ICMP. The captured packets can be written to a file or standard output. One of the most powerful features of the tcpdump command is its ability to use filters and capture only the data you wish to analyze. prints out a description of the contents of packets on a network interface.

j. **nagios**:

Nagios is an open source host, service and network monitoring program. It monitors specified hosts and services, alerting you to any developing issues, errors or improvements. It is used for the monitoring of network services (SMTP, POP3, HTTP, NNTP, PING, etc. and monitoring of host resources (processor load, disk usage, etc.), Ability to define network host hierarchy using "parent" hosts, allowing detection of and distinction between hosts that are down and those that are unreachable, Contact notifications when service or host problems occur and get resolved (via email, pager, or user-defined method), Automatic log file rotation.

i. **Zabbix**:

Zabbix is a full-featured monitoring solution for larger networks. It can discover all kind of networking devices using different methods, check machine states and applications, sending pre-defined alarm messages and visualize complex data correlations. Supports comprehensive monitoring, alerting, trend analysis, and visualization of performance metrics.

k. **nmap**:

Network exploration tool and security / port scanner. Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the “interesting ports table”.

l. **w**:

Show who is logged on and what they are doing. w displays information about the users currently on the machine, and their processes.  The header shows, in this order, the current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes. The following entries are displayed for each user: login name, the tty name, the remote host, login time, idle time, JCPU, PCPU, and the command line of their current process. The JCPU time is the time used by all processes attached to the tty. It does not include past background jobs, but does include currently running background jobs. The PCPU time is the time used by the current process, named in the "what" field.

M. **ps**:

Reports a snapshot of the current processes. ps displays information about a selection of the active processes.  If you want a repetitive update of the selection and the displayed information

**QUESTION 2**

- **EnCase Forensic:**

*Evidence Gathering:* Using EnCase Forensic, detectives can gather digital evidence from a variety of sources, including PCs, mobile devices, cloud storage, Evidence Gathering: Using EnCase Forensic, detectives can gather digital evidence from a range of devices, including laptops, smartphones, cloud storage, and network shares.

*Data analysis:* It offers strong tools, such as file system analysis, registry analysis, timeline analysis, and keyword searches, for evaluating gathered data.

*Evidence Preservation*: EnCase Forensic maintains a clear chain of custody by guaranteeing the integrity and preservation of digital evidence throughout the course of the inquiry.

Reporting: It provides thorough reporting features to record conclusions and provide evidence in an intelligible manner, which is frequently necessary for court cases.

*Installation Process:*

Acquire License: Obtain a license for EnCase Forensic from OpenText. This usually involves purchasing a license based on the number of users and desired features.

Reporting: It provides thorough reporting features to record conclusions and provide evidence in an intelligible manner, which is frequently necessary for court cases.

Installation: Run the installation wizard, which guides you through the process of installing the software on your system. This typically involves selecting installation options, specifying installation directory, and configuring any necessary settings.

License Activation: Use the OpenText-provided license key to activate the program after installation. By taking this step, you can be sure that your license to use the product is valid.

Update: To make sure you have the most recent features and security patches, it is advised that you search for and install any available updates.

Stressing the Value of Open Source: Although EnCase Forensic is a popular and effective tool in the field of digital forensics, the availability of open-source substitutes is as important.

Transparency: The forensic community may confirm the software's correctness and dependability by looking at the source code, which is made possible by open-source tools.

Cost-Effectiveness: Individuals and businesses with tight budgets can utilize several open-source forensic tools because they are freely available.

Community Collaboration: The forensic community benefits from the open-source model's promotion of creativity and collaboration, which results in the creation of new instruments and methods to deal with new problems.

A few well-known open-source digital forensic programs are bulk extractor, Volatility, The Sleuth Kit (TSK), and Autopsy. These technologies supplement proprietary products like EnCase Forensic with strong capabilities for gathering, analyzing, and reporting digital evidence.

- **Helix**

It is an open-source digital forensic tool made to help detectives gather and examine digital evidence. Like EnCase Forensic and other proprietary forensic tools, it offers several capabilities, but it is free to use and based on open-source software components. An outline of its features, how to install it, and why it's open-source are provided below:

*Functions of Helix Forensic Tool:*

Helix facilitates live examination of operating systems, allowing investigators to collect transient data about open files, network connections, and running processes without affecting the system's state.

Disk imaging: It makes forensic disk images easier to create by collecting all the contents of storage devices in a way that adheres to forensic best practices, all the while protecting data integrity and upholding a clear chain of custody.

Data Recovery: Helix has methods for retrieving erased files and partitions, which can assist investigators in finding potentially important evidence that a user may have mistakenly or purposely erased.

Data Analysis: To find pertinent information and patterns, it offers capabilities for analyzing disk pictures and extracted data, such as timeline analysis, keyword searching, metadata extraction, and file system analysis.

Reporting: Helix can provide thorough forensic reports that include conclusions, methods of analysis, and presentations of the evidence. These reports are crucial for court processes.

*Procedure for Installation:*

Get the Helix ISO image from reliable sources or the official website.

Make Bootable Media: Use a program like Rufus or UNetbootin to make a bootable USB device or burn the Helix ISO image to a CD or DVD.

Boot from Media: To boot from the bootable media, place it into the intended system and insert it. Changing the system BIOS/UEFI settings' boot order may be necessary to do this.

Start Helix: After the system has booted up, a graphical or command-line interface including several forensic tools and utilities will be available to you.

Set Up Tools: Learn how to use the various tools and set them up according to the needs of your research.

Conduct Forensic Analysis: In accordance with accepted forensic practices, gather, examine, and record digital evidence using Helix tools.

*Significance of Open Source:*

Helix's open-source design provides several benefits.

Transparency: To guarantee transparency and confirm the quality and dependability of the product, users can examine the source code.

Community Collaboration: By enabling users to report defects, offer new features, and make changes, the open-source model encourages creativity and collaboration within the forensic community.

Cost-Effectiveness: Since Helix is open source, even individuals and small businesses with tight resources can use it. This encourages a broader use of digital forensics standard practices and lowers the entrance barrier for forensic investigations.

Investigators can do comprehensive and transparent digital evidence investigations, bolstering the integrity and admissibility of conclusions in judicial processes, by utilizing open-source forensic tools such as Helix.

- **Backtrack**:

A Linux distribution designed with digital forensics and penetration testing in mind. It's a popular option for forensic investigations even if it's not just a forensic tool because it comes with a lot of forensic utilities and features. An outline of its features, how to install it, and why it's open-source are provided below:

*Features of the Forensic Tools BackTrack (Kali Linux):*

Real-time analysis Backtrack facilitates real-time examination of operating systems, allowing detectives to collect sensitive information about active processes, open files, and network connections without compromising the system's condition.

Disk imaging: It makes forensic disk images easier to create by collecting all of the contents of storage devices in a way that adheres to forensic best practices, all the while protecting data integrity and upholding a clear chain of custody.

Data recovery: BackTrack has tools for retrieving erased files and partitions, which can assist investigators in finding potentially important evidence that a user may have mistakenly or purposely erased.

Data Analysis: To find pertinent information and patterns, it offers capabilities for analyzing disk pictures and extracted data, such as timeline analysis, keyword searching, metadata extraction, and file system analysis.

Network Forensics: BackTrack's tools for packet capture, protocol decoding, and network traffic analysis enable investigators to examine network activity and spot potentially suspicious activities or security breaches.

Reporting: BackTrack offers capabilities for generating detailed forensic reports documenting findings, analysis methodology, and evidence presentation, which are essential for legal proceedings.

*Installation Process:*

Download BackTrack (Kali Linux): Obtain the BackTrack (Kali Linux) ISO image from the official website or reputable sources.

Create Bootable Media: Burn the BackTrack (Kali Linux) ISO image to a CD/DVD or create a bootable USB drive using software like Rufus or UNetbootin.

Boot from Media: Insert the bootable media into the target system and boot from it. This may involve changing the boot order in the system BIOS/UEFI settings.

Install BackTrack (Kali Linux): Follow the on-screen prompts to install BackTrack (Kali Linux) onto the target system. You may choose to install it alongside existing operating systems or use it as a standalone OS.

Configure Tools: Once installed, familiarize yourself with the available forensic tools and utilities included in BackTrack (Kali Linux) and configure them as needed for your investigation.

Perform Forensic Analysis: Utilize the forensic tools and utilities provided by BackTrack (Kali Linux) to collect, analyze, and document digital evidence according to standard forensic procedures.

*Significance of Open Source:*

The open-source nature of BackTrack (Kali Linux) offers several advantages:

Transparency: Users can inspect the source code to ensure transparency and verify the accuracy and reliability of the software.

Community Collaboration: The open-source model fosters collaboration and innovation within the forensic community, allowing users to contribute improvements, report bugs, and suggest new features.

Cost-Effectiveness: BackTrack (Kali Linux) is freely available, making it accessible to individuals and organizations with limited budgets. This lowers the barrier to entry for forensic investigations and promotes wider adoption of best practices in digital forensics.

The integrity and admissibility of results in court proceedings can be supported by investigators conducting comprehensive and transparent examinations of digital evidence using open-source forensic tools like BackTrack (Kali Linux).

- **Autopsy**

An open-source digital forensic platform that serves as one such substitute. We will talk about its features, how to install it, and why it is open-source.

*The purposes of autopsies Forensic Investigators can produce forensic disk pictures of storage devices using Autopsy, a forensically sound method of retaining the original data.*

Data recovery: It provides investigators with the means to recover erased files and partitions, which may include evidence that is pertinent to their case.

Autopsy makes it easier to search for keywords across disk pictures, which helps investigators find files and objects of interest rapidly.

File System Analysis: It offers thorough file system analysis, which includes timeline analysis to retrace user behavior, metadata extraction, and file classification.

Artifact examination: To gain insights into user behavior, Autopsy facilitates the examination of a variety of artifacts, including chat logs, email headers, registry entries, and internet history.

Reporting: It offers capabilities for generating comprehensive forensic reports documenting findings, analysis methodology, and evidence presentation.

*Installation Process:*

Download Autopsy: Obtain the Autopsy installer package from the official website or reputable sources.

Install Autopsy: Run the installer package and follow the on-screen prompts to install Autopsy on your system. The installation process typically involves selecting installation options, specifying installation directory, and configuring any necessary settings.

Launch Autopsy: Once installed, launch Autopsy from the installed location or desktop shortcut. The software will open in a web browser interface.

Create Case: Start by creating a new case within Autopsy and specifying the disk image or data source to be analyzed.

Analyze Data: Use Autopsy's tools and modules to analyze the data, perform keyword searches, examine file system structures, and explore artifacts relevant to the investigation.

Generate Reports: After analysis is complete, generate forensic reports within Autopsy summarizing the findings and analysis results.

*Significance of Open Source:*

Autopsy being open source offers several advantages:

Transparency: Users can inspect the source code to ensure transparency and verify the accuracy and reliability of the software.

Community Collaboration: The open-source model fosters collaboration and innovation within the forensic community, allowing users to contribute improvements, report bugs, and suggest new features.

Cost-Effectiveness: Autopsy is freely available, making it accessible to individuals and organizations with limited budgets. This lowers the barrier to entry for forensic investigations and promotes wider adoption of best practices in digital forensics.

By leveraging open-source forensic tools like Autopsy, investigators can conduct thorough and transparent examinations of digital evidence, supporting the integrity and admissibility of findings in legal proceedings.

- **Anadisk**

It is mostly used to examine floppy disks and disk images. Its purpose is to reveal details about the data stored on disk pictures by extracting information from them. Let's examine its features, how to install it, and why it is open-source:

*Anadisk's functions include disk image analysis, which enables users to examine disk images from a variety of sources, such as hard drives, floppy disks, and disk image files.*

File System Examination: FAT12, FAT16, and FAT32 file systems—which are frequently found on floppy disks and other outdated storage devices—can all be examined within disk images.

File Extraction: With Anadisk, users can retrieve specific data saved in disk images by extracting files and directories from the image.

Data Recovery: Although its functionality in this area may be constrained in comparison to more sophisticated forensic tools, it offers users basic data recovery capabilities, enabling them to recover deleted files or partitions from disk images.

File System Examination: It supports the examination of file systems within disk images, including FAT12, FAT16, and FAT32 file systems commonly found on floppy disks and older storage devices.

File Extraction: Anadisk enables users to extract files and directories from disk images, allowing for the retrieval of specific data stored within the image.

Data Recovery: It provides basic data recovery capabilities, allowing users to recover deleted files or partitions from disk images, though its functionality in this regard may be limited compared to more advanced forensic tools.

File System Information: Anadisk can display detailed information about the file system structure, including file allocation tables (FAT), directory entries, and file attributes.

Checksum Verification: It supports checksum verification to ensure the integrity of disk images and verify that they have not been altered or corrupted.

*Installation Process:*

Download Anadisk: Obtain the Anadisk software package from the official repository or reputable open-source software distribution platforms.

Extract Files: If the Anadisk package is compressed (e.g., in a ZIP file), extract the contents to a directory on your system.

Compile (if necessary): Depending on the distribution and format of the Anadisk software, you may need to compile it from source code. Follow the instructions provided in the software documentation or README file for compiling the software.

Run Anadisk: Once the software is installed or compiled, you can run Anadisk from the command line or graphical user interface, depending on the available interface options.

Load Disk Image: Use Anadisk to load the disk image you want to analyze. Specify the path to the disk image file as a command-line argument or navigate to the file using the graphical interface.

Analyze Disk Image: Once the disk image is loaded, you can start analyzing its contents using the various functions and tools provided by Anadisk.

*Significance of Open Source:*

Anadisk being open source offers several advantages:

Transparency: Users can inspect the source code to understand how the software works and verify its reliability and accuracy.

Community Collaboration: The open-source model fosters collaboration among developers and users, allowing for contributions, feedback, and improvements to the software.

Accessibility: Open-source software is freely available, making it accessible to users regardless of their financial resources or location.

By leveraging open-source forensic tools like Anadisk, users can conduct disk image analysis and data extraction tasks effectively while benefiting from transparency, community collaboration, and accessibility.

- **CopyQM Plus**

A proprietary disk imaging and cloning software developed by Qiao Mu Software. As such, it is not open source. However, I can provide information about its functions and installation process, though I won't be able to emphasize its open-source nature as it's not applicable.

*Functions of CopyQM Plus:*

Disk Imaging: Hard drives, floppy disks, and other storage media can all be precisely duplicated or imaged using CopyQM Plus. The original disk's contents can then be replicated or saved in these disk images for future use.

Disk Cloning: It allows users to copy entire disks or certain partitions to different drives. System migration, updating storage devices, and making duplicate disks of current disks can all benefit from this feature.

Data Transfer: CopyQM Plus facilitates the transfer of data between disks, partitions, or disk images. Users can copy individual files, directories, or entire disk structures with ease.

Data Recovery: Although its skills in this area may be restricted when compared to specialized data recovery software, CopyQM Plus can occasionally be used for simple data recovery tasks, such as retrieving deleted files or partitions.

Disk Management: It provides basic disk management functions, allowing users to format disks, create or delete partitions, and manage disk structures.

*Installation Process:*

Download CopyQM Plus: Visit the official website of Qiao Mu Software or authorized distributors to obtain the CopyQM Plus software package.

Run Installer: Double-click the installer executable file to launch the installation wizard.

Follow Installation Instructions: Follow the on-screen instructions provided by the installation wizard. This typically involves accepting the software license agreement, choosing the installation directory, and selecting any additional options or components to install.

Complete Installation: Once the installation process is complete, you may be prompted to restart your computer to finalize the installation.

Launch CopyQM Plus: After installation and reboot, you can launch CopyQM Plus from the Start menu, desktop shortcut, or installation directory.

Activate License (if required): Depending on the licensing model used by CopyQM Plus, you may need to activate your license using a license key or activation code. Follow the instructions provided with your license to complete the activation process.

*Emphasizing Open Source (Not Applicable):*

As mentioned earlier, CopyQM Plus is not open source. It is proprietary software developed and maintained by Qiao Mu Software. Therefore, it does not have the benefits typically associated with open-source software, such as transparency, community collaboration, and accessibility of source code.

**QUESTION 3**

Five forensics tools suitable for live systems and network operations, discussing their configurations for these specific tasks are;

**WIRESHARK**

*Function:*

Network Traffic Capture and Analysis: Wireshark is a powerful open-source network protocol analyser. It allows users to capture and analyse network traffic in real-time. Wireshark can dissect and display the details of packets, making it invaluable for network troubleshooting, protocol analysis, and security monitoring.

*Configuration:*

Live Packet Capturing: Users can configure Wireshark to capture live network traffic. This involves selecting the network interface from which to capture packets. Configuration may include setting filters to capture specific types of traffic or specifying capture options such as packet size limits.

**VOLATILITY**

*Function:*

Memory Forensics: Volatility is an open-source memory forensics framework. It is used to analyse memory dumps of live systems, extracting information about running processes, network connections, and system state from volatile memory.

*Configuration:*

Memory Image and Profile Specification: To use Volatility, analysts typically provide a memory image file (captured from a live system) and specify the profile that corresponds to the operating system and version. Configuration involves selecting the appropriate plugins for analysis based on the type of information needed.

**LIVE RESPONSE COLLECTION (LRC) TOOLS (E.G., CROWDSTRIKE FALCON):**

*Function:*

Real-time Incident Response: LRC tools like CrowdStrike Falcon are designed for real-time incident handling and response. They provide capabilities for live forensics, threat detection, and response to security incidents.

*Configuration:*

Tool-Specific Configuration: The configuration of LRC tools varies depending on the specific tool used. Configuration options may include setting up real-time monitoring, defining response actions for

different types of incidents, and configuring alerting mechanisms. Specific details depend on the features and capabilities of the chosen LRC tool.

**BRO (ZEEK):**

*Function:*

Network Analysis Framework: Bro, now known as Zeek, is a powerful network analysis framework. It captures, logs, and organizes network traffic, providing insights into network behavior. It goes beyond simple packet capture, enabling the creation of custom network policies and rules.

*Configuration:*

Defining Network Policies and Rules: Configuration involves specifying policies and rules to define what types of network activities should be monitored and logged. Users can customize Bro's behavior based on the specific network environment and security requirements.

**SNORT:**

*Function:*

Intrusion Detection System (IDS): Snort is an open-source intrusion detection system that monitors network traffic for suspicious activities or patterns indicative of a security threat. It can be deployed in real-time to detect and respond to potential intrusions.

*Configuration:*

Rules and Policies Setup: Configuration in Snort involves defining rules and policies to identify and respond to specific types of network traffic. Users configure rules to detect known attack patterns or unusual behavior. Additionally, configuration may include specifying response actions for detected threats.

**QUESTION 4**

Core forensic commands and their importance;

I. **DD (DISK DUMP):**

Importance: Creates forensic copies (images) of storage media for analysis without altering the original data.

II. **HASHDEEP:**

Importance: Computes hash values (MD5, SHA-1, SHA-256) to verify the integrity of files during forensic analysis.

III. **FILE:**

Importance: Determines file type and metadata, aiding in the identification of unknown files.

IV. **STRINGS:**

Importance: Extracts readable text from binary files, helping to identify relevant information within them.

V. **GREP:**

Importance: Searches for specific patterns or keywords within files, facilitating the identification of relevant information.